

# **CYBER SECURITY INTERNSHIP REPORT AT SHADOWFOX**

NAME:- Aniket Ramesh Chavan

BATCH :- july2025

MAIL ID :- [chavananiket5222@gmail.com](mailto:chavananiket5222@gmail.com)

TASK LEVEL :- Beginner

## **BEGINNER LEVEL TASK**

1: - Find all the ports that are open on the website  
<http://testphp.vulnweb.com/>

## **REPORT OF TASK LEVEL**

### **Introduction :-**

Cyber security is now spreading in all over internet due to security and risks on the internet . websites are vulnerable due to is structure , security and build up . so here following a Way to identifying the website in vulnerable or not using scaning the open ports using tools and some tricks.

Website :- [testphp.vulnweb.com](http://testphp.vulnweb.com)

## **1. Port scanning :-**

In port scanning we are checking the port of the website which is opened or not. Because most of the websites are compromised due to open ports. Ports are vulnerable and easy to access the websites.

### **Task 1**

**Find all the ports that are open on the website**  
**<http://testphp.vulnweb.com/>**

- **Attack Name :-** Port Scanning
- **Severity :-** High and its score 7.0 – 8.9

### **❖ Steps to reproduce with screenshot**

Step 1 :- ip address identification:-

In this technique I used nslookup tool to identify the ip of the given website. Ip address is a unique protocol used for internet services. Targeting the ip is our goal.

Command :- `nslookup testphp.vulnweb.com`

Step 2 :- port scanning :-

In port scanning we are checking the port of the website which is opened or not.

I used nmap tool to scan the ports are opened or not

Command :- `nmap -p- testphp.vulnweb.com`

Here is result of port scanning

Website :- testphp.vulnweb.com

Ip address :- 44.228.249.3

Nmap command :- `nmap -p- 44.228.249.3`

### **Analysis :-**

**Port / protocol** :- 80/tcp

**State** :- open

**Service** :- http

**Version** :- nginx 1.19.0

Port 80 / tcp host is active http services . this web server using nginx 1.19.0 version tho secure the site update and upgrade the site with reguraly security patches .

Step 3 :- port scanning fig :-

```
(aniket@Aniket1Monly)-[~]
$ nslookup testphp.vulnweb.com
Server:
192.168.230.2
Address:
192.168.230.2#53

Non-authoritative answer:
Name: testphp.vulnweb.com
Address: 44.228.249.3
Name: testphp.vulnweb.com
Address: 64:ff9b::2ce4:f903

(aniket@Aniket1Monly)-[~]
$ nmap -p- 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-31 19:13 IST
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 52.47% done; ETC: 19:17 (0:01:32 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00023s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident

Nmap done: 1 IP address (1 host up) scanned in 222.74 seconds

(aniket@Aniket1Monly)-[~]
$ nmap -p- testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-31 19:21 IST
Stats: 0:10:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.94% done; ETC: 19:36 (0:04:43 remaining)
Stats: 0:10:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.94% done; ETC: 19:36 (0:04:43 remaining)
Stats: 0:19:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.70% done; ETC: 19:43 (0:02:42 remaining)
Stats: 0:19:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.73% done; ETC: 19:43 (0:02:42 remaining)
Stats: 0:19:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.77% done; ETC: 19:43 (0:02:42 remaining)
Stats: 0:19:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.84% done; ETC: 19:43 (0:02:41 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.00025s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65532 filtered tcp ports (no-response)
```

Fig :- nmap scanning

## ❖ Impact :-

Advantages :-

🔍 Finds Websites or Web Services :-

Port 80 is where most websites live. Scanning it helps you find if a website or web service is running.

🔍 Not Very Suspicious :-

port 80 is commonly used, scanning it doesn't usually raise red flags in firewalls or security systems.

Disadvantages :-

🔍 Might Still Be Noticed While it's less obvious than other scans, if you scan too many times or too fast, you might still get caught.

## ❓ Limited Info

Just knowing port 80 is open doesn't tell you much unless you look deeper into what's running on it.

## ❖ Mitigation steps :-

1. Block or limit access to port 80 from unknown or untrusted IPs. Only allow trusted users or networks to reach your web server.
2. Set Up Intrusion Detection/Prevention Systems (IDS/IPS)  
Tools like Snort, Suricata, or cloud-based security services can detect and block scanning attempts.  
They can alert you if someone is probing your port 80 repeatedly.
3. Always check the url and https or http protocol port 80
4. Set a limit access to directories and authentications always check the system data is encrypted and safe
5. Update security patches and keep system updated .

## ❖ Resources used :-

Kali linux operating system , nmap tool ( for scanning open ports ), nslookup tool ( for ip address identify )

